транспортного предприятия, определить показатели качества транспортного обслуживания (требования к обслуживанию), а затем определить зависимости. Предполагается получение зависимостей между показателями работы транспортного предприятия (водителей, транспортных средств), затратами на транспортное обслуживание и требованиями к обслуживанию логистической системы.

Список литературы: 1. Альбеков А.У., Федько В.П., Митько О.А. Логистика коммерции. – Ростов-на-Дону: Феникс, 2001. – 512 с. 2.Модели и методы теории логистики: 2-е изд. / Под ред. В.С. Лукинского. – СПб.: Питер, 2008. – 448 с. 3.Бауэрсокс Д. Дж., Клосс Д. Дж. Логистика: интегрированная цепь поставок / Пер. с англ. – М.: ЗАО «Олимп-бизнес», 2001. – 640 с. 4.Сергеев В.И. Логистика в бизнесе. – М.: ИНФРА-М, 2001. – 608с. 5. Д. Джонсон, Д. Вуд, Д. Вордлоу, П. Мерфи мл. Современная логистика, 7-е изд.: Пер. с англ. – М.: ИД «Вильямс», 2004. – 624 с. 6. Логистика: управление в грузовых транспортно-логистических системах. Под ред. Л. Б. Миротина. – М.: Юристъ, 2002. – 414 с. 7.Единая транспортная система. В.Г. Галабурда, В.А. Персианов, А.А. Тимошин и др./ Под ред. В.Г. Галабурды. 2-ое изд. с измен. и дополн. – М.: Транспорт, 2001. – 303 с. 8. Смехов А.А. Основы транспортной логистики. – М.: Транспорт, 1995. – 197 с. 9. Вентцель Е.С. Исследование операций. Задачи, принципы, методология / Е.С. Вентцель. – 4-е изд., стереотип. – М.: Дрофа, 2006. – 206 с. 10. Бутаев Ш.А., Мадаминов Ю. Совершенствование методов управления процессами автомобильных перевозок грузов. – Ташкент: Фан, 1988. – 152 с. 11. Дикий С.О. Побудова комплексної моделі функціонування АТП багатоаспектної діяльності. Вісник. Збірник наукових праць Транспортної академії України та Українського транспортного університету. – К., РВВ УТУ, 1999. Вип. 3. – 124-127 с. 12. Бідняк М.Н. Формування і реалізація мінімального об’єму транспортних послуг. Вісник. Збірник наукових праць Транспортної академії України та Українського транспортного університету. – К.: РВВ УТУ, 1999, Вип. 3. – 100-107 с. 13. Нагорний Є.В., Шраменко Н.Ю. Методика вибору оптимальної стратегії поведінки суб’єктів транспортного ринку в умовах конкуренції. Сборник научных трудов. Автомобильный транспорт. Вып. №9. – ХНАДУ, 2006. – 127-132 с. 14. Вельможин А.В., Гудков В.А, Миротин Л.Б., Куликов А.В. Грузовые автомобильные перевозки.– М.: Горячая линия «Телеком», 2006. – 506 с.

Поступила в редколлегию 20.02.2009

УДК 681.32

САПРЫКИН А.С., БОЧАРНИКОВА М. В., АДАМОВ А. С., ХНУРЭ

МЕТОДИКА ОЦЕНКИ УБЫТКОВ ПРЕДПРИЯТИЯ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

В данной работе проанализирована проблема влияния вредоносных программ на деятельность предприятия и разработана методика подсчета экономического ущерба вследствие их деструктивного действия.

1. Введение

Реалии современного мира экономики таковы, что в условиях агрессивной рыночной среды практически любая компания постоянно сосредоточена на поддержании своей конкурентоспособности. И акцент здесь все больше

смещается от конкурентоспособности продуктов или услуг к конкурентоспособности компании в целом. Очевидно, что основным инструментом ее поддержания является стратегическое бизнес-планирование, направленное на развитие ее адаптивности и повышение устойчивости к воздействию рыночной среды.

Одним из критериев, определяющих финансовую устойчивость компании, являются темпы роста прибыли, опережающие темпы роста затрат на содержание компании. Главная цель любого коммерческого предприятия – получение прибыли и ее максимизация. С экономической точки зрения прибыль - это разница между денежными поступлениями и денежными выплатами. Если эта разница оказывается отрицательной, то предприятие убыточно. Чтобы увеличивать прибыль, руководство стремится минимизировать издержки.

Следовательно, из-за того, что могут возникнуть непредвиденные затраты: влияние вредоносных программ, утечка информации, атаки на компьютерную сеть, предприятие недополучит планируемые финансовые поступления, понесет убытки, может потерять ценных клиентов, деловых партнеров, они с опасением будут относиться к предприятию, которое не может защитить себя от подобных атак [1].

Увеличение количества персональных компьютеров, рост пропускных способностей коммуникационных каналов ведет к тому, что масштабы вирусных эпидемий, а соответственно, и потери от них, растут с каждым годом, поэтому руководству компаний необходимо достаточно серьезно и ответственно подходить к вопросам информационной безопасности своего предприятия.

В современном мире стремительное развитие информационных технологий приводит к более эффективной работе всех структур и подразделений предприятий, но в тоже время с каждым днем увеличивается вероятность проникновения вредоносных программ в компьютерную систему, что может повлечь за собой не только кратковременные сбои в сети, но и полную остановку деятельности предприятия. Убытки, наносимые вредоносными программами по всему миру, исчисляются миллиардами долларов и продолжают ежегодно расти. Деструктивное действие вирусных технологий ощущают как крупные компании, так и компании, среднего бизнеса, где информационной безопасности уделяется достаточно мало внимания, а число компьютеров постоянно увеличивается [2].

2. Цель и задачи исследования

Целью и задачей исследования является разработка методики оценки ущерба от распространения деструктивных вирусных технологий в компьютерных сетях предприятий. Объектом исследования служит структура экономических взаимоотношений всех субъектов предпринимательской деятельности рынка, а субъектом выступает деятельность отдельных предприятий.

3. Разработка методики оценки ущерба от распространения деструктивных вирусных технологий в компьютерных сетях предприятий

С экономической точки зрения деятельность любого предприятия можно представить в виде набора показателей, профессионально оценивая которые можно с определенной долей вероятности судить о настоящем положении дел на

этом предприятии и делать необходимые прогнозы на будущее. Набор этих показателей (показатели ликвидности, рентабельности, устойчивости, показатели производительности труда, роста объема производства, количества затрат и др.) в совокупности дает возможность сделать очень качественную комплексную оценку и характеристику финансового состояния. Объединяя эти показатели в одну многофакторную модель с помощью статистических данных за как можно больший промежуток времени можно выявить закономерности и зависимости, анализируя которые в будущем можно судить об изменениях в работе предприятия. Эти изменения могут происходить как в сторону улучшения конечного финансового результата, так и соответственно его ухудшения и являться следствием воздействия различных внутренних и внешних факторов, наша задача состоит в том, чтобы определить воздействие именно компьютерных вирусных технологий и оценить ущерб от их деструктивной активности. Эти изменения носят разносторонний характер, что связано со спецификой отраслей экономики, с текущими особенностями действующих предприятий, с состоянием экономической среды, в которой они работают.

На рисунке 1 представлена модель финансового ущерба, которая имеет следующий вид:

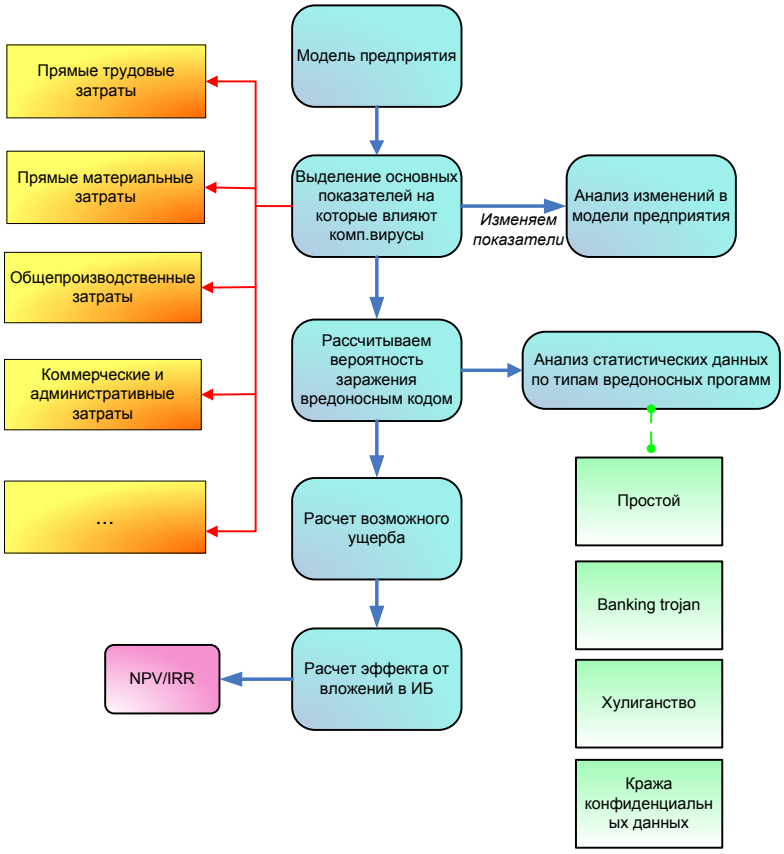

Рис 1. Модель расчета финансового ущерба

Финансовые потери, которые несут предприятия от вирусных атак можно представить следующим образом [3]:

- при ведении электронной коммерции потери, связанные с простоем и выходом из строя сетевого оборудования;
- нанесение ущерба имиджу и репутации компании;

- оплата сверхурочной работы ИТ-персонала и/или оплата работ подрядчикам, которые занимались восстановлением корпоративной информационной системы;
- оплата консультаций внешних специалистов, которые осуществляли восстановление данных, выполняли ремонт и оказывали юридическую помощь;
- оплата ремонта физических повреждений от виртуальных атак;

Чтобы рассчитать потери компании от вирусов (ML), необходимо разделить их на несколько составляющих в зависимости от характера их воздействия на деятельность предприятия:

- сбои (полная остановка работы) в работе компьютеров. Здесь учитывается кол-во компьютеров (шт.), время наладки 1-го компьютера (ч), стоимость наладки (почасовая или в зависимости от сложности);
- мошенничество, кража денег со счетов: количество существующих счетов-депозитов, сумма средств на счетах;
- хулиганство (вирусы, которые мешают работать, отвлекают, засоряют компьютер): кол-во потраченного рабочего времени (ч) в сутки.

Информационную безопасность предприятия представим в виде следующей структуры [4]:

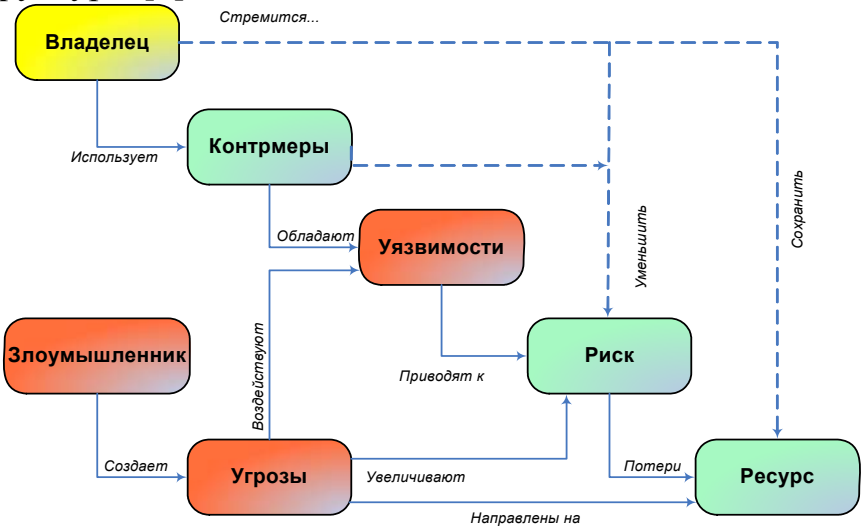

Рис. 2 – Модель информационной безопасности

При расчете эффективности инвестиций в информационную безопасность можно использовать следующие формулы.

Net Present Value, NPV - накопленный дисконтированный эффект за расчетный период. NPV рассчитывается по формуле:

$$\mathrm{NPV} = \sum_{m=0}^{K} ДП_m * \alpha_m(E)$$

где $\alpha_m = \frac{1}{(1+E)^{t_m - t^0}}$ - коэффициент дисконтирования на m-м шаге,

tm - момент окончания m-го шага (в годах),

$ДП_m$ – денежный поток на m-м шаге,

k – количество шагов.

Для признания проекта эффективным необходимо, чтобы NPV проекта был положительным.

- Внутренняя норма доходности (Internal Rate of Return, IRR).
- Внутренняя норма доходности определятся как такое положительное число Ев, что при норме дисконта E = Ев величина NPV(чистый дисконтированный доход) обращается в 0, при всех больших значениях E - отрицательна, при всех меньших значениях E - положительна. Если не выполнено хотя бы одно из этих условий, считается, что ВНД не существует.
- Проекты, у которых IRR > E, имеют положительный NPV и поэтому эффективны.
- Проекты, у которых IRR< E, имеют отрицательный NPV и поэтому неэффективны [5].

Главным фактором, который непосредственно оказывает прямое влияние на размер ущерба от вредоносных программ, является простой компьютерной сети. За период времени, в течение которого предприятие не имеет возможности осуществлять свою деятельность в полном объеме, оно терпит убытки, что в последствии выражается в ухудшении всех финансово-экономических показателей ее деятельности. Немаловажными факторами являются также потери ценной информации и ухудшение имиджа фирмы, что выражается в невозможности противостоять вирусным атакам.

Выделим следующие составляющие показателей деятельности и элементы возникающих затрат, которые напрямую позволяют оценить величину ущерба от простоя сети, а именно: затраты времени специалистов на устранение вредоносной программы; стоимость утраченных данных; расходы на аппаратно-технические средства и программное обеспечение; простой системы; потери рабочего времени сотрудников из-за простоя системы; снижение производительности труда; ущерб, нанесенный деловой репутации пострадавшей фирмы.

$$\text{ПРОСТОЙ} = (\text{comp\_num} \times \text{fix\_time} \times \text{adjuster\_hour\_payment}) + \text{additional\_expences} +$$
$$+\left(\frac{\text{items\_day} \times \text{product\_price} \times \text{fix\_time} \times \text{comp\_num}}{8 \times \text{adjuster\_num}}\right) + \left(\frac{\text{salary} \times \text{comp\_num} \times \text{fix\_time}}{8 \times 22 \times \text{adjuster\_num}}\right)$$

Где comp_num – количество компьютеров в офисе;

fix_time – время, необходимое специалисту на наладку одного компьютера (ч);

adjuster_hour_payment – стоимость одного часа работы наладчика;

adjuster_num – количество специалистов - наладчиков;

additional_expences - дополнительные затраты на восстановление сети и покупку оборудования;

product_price – стоимость одной единицы выпускаемой продукции;

items_day – кол-во выпускаемых единиц продукции в день;

salary – заработная плата одного работника в месяц;

Также нетрудно вычислить изменения производительности труда (количество произведенной продукции по отношению к средней численности сотрудников), связанные с недозагрузкой рабочего персонала.

Была написана программа, которая, при введении определенных экономических показателей деятельности предприятия считает, каким образом отразились на ее деятельности сбои компьютерной сети.

4. Экспериментальные исследования

На примере компании «Лаборатория Дизайн и Тест» проведем соответствующие расчеты.

«Лаборатория Дизайн и Тест» - это исследовательский и аналитический центр, который организован с целью анализа и противодействия вредоносному коду. Компания сотрудничает с Лабораторией Касперского с 2005 года. Главный офис компании расположен в г. Харькове. В Лаборатории работают 10 аналитиков с уникальным опытом работы в исследовании вредоносного кода. Аналитики сделали уже более 5000 экспертных заключений на вредоносные программы для различных платформ Microsoft Windows 98/Me/2000/XP/2003, Linux, WinMobile, MacOS [6].

Организационная структура компании имеет следующий вид, который представлен на рис. 3:

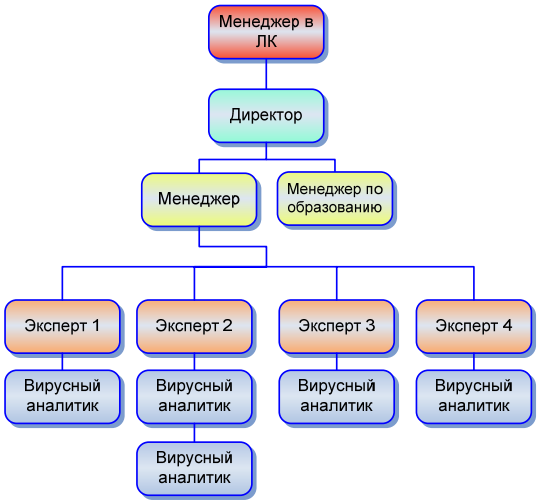

Рис. 3 – Организационная структура компании

Интерфейс программы с расчетами представлен на рис.4:

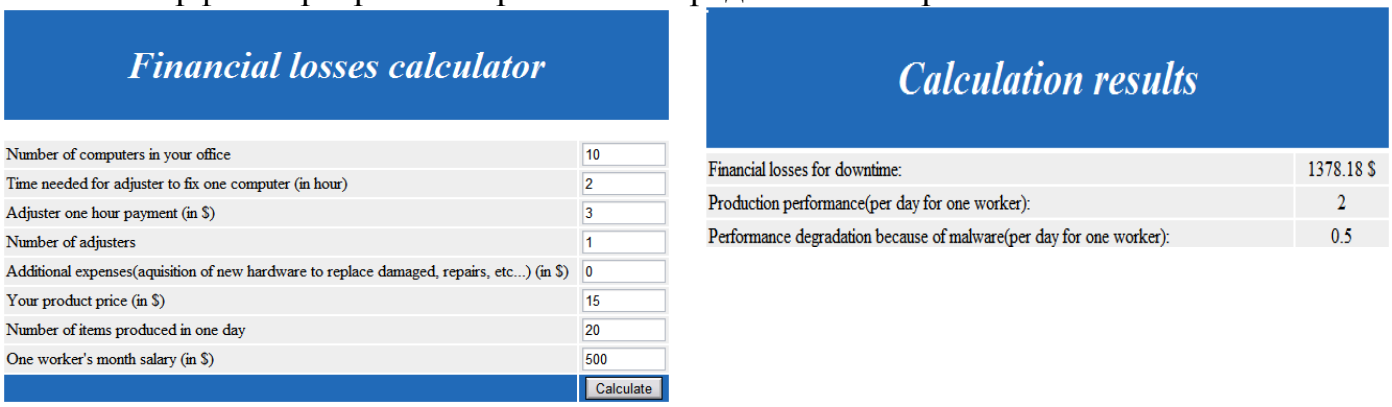

Рис. 4 – Интерфейс программы

5. Выводы

Деструктивное действие вредоносных программ на деятельность предприятия проявляется в уменьшении прибыли за отчетный период, ухудшении имиджа и репутации компании и других негативных последствиях. Чтобы показать предприятиям возможные последствия разработана система подсчета финансовых потерь от простоя компьютерной сети. Данная система позволяет дать качественную оценку производительности труда и оценить убытки компании от действия вредоносных программ. Также в программе предусмотрено сохранение результатов расчетов в базу данных для дальнейшего анализа работы предприятия.

Список литературы: 1. О. К. Филатов, Л. А. Козловских, Т. Н. Цветкова Планирование, финансы, управление на предприятии. Практическое пособие. - Финансы и статистика, 2005г. – 384 с. 2. www.viruslist.ru. 3. Бочарникова М.В., Сапрыкин А.С. Разработка методики оценки ущерба от распространения вирусных технологий на действующих предприятиях, студенческая конференция IT Security for new generation, Москва 28 – 29 августа 2008 г. 4. Бочарникова М.В., Сапрыкин О.С., Україна, Харків Економічні інструменти інформаційної безпеки виробничих та підприємницьких структур в сучасних умовах. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я XVI міжнародна конференція Харків, 4-6 червня 2008. 5. Селезнева Н.Н., Ионова А.Ф. Финансовый анализ. Управление финансами: Учеб. пособие для вузов.- 2-е изд. – М.: ЮНИТИ-ДАНА, 2003. – 639 с. 6. http://www.dnt-lab.com

Поступила в редколлегию 25.12.2008

УДК 622.692.4

Л. М.ЗАМІХОВСЬКИЙ, С.О. САПРИКІН, *УкрНДІгаз, м. Харків*

КОНЦЕПЦІЯ МОНІТОРИНГУ ТЕХНІЧНОГО СТАНУ ГАЗОПЕРЕКАЧУВАЛЬНОГО ОБЛАДНАННЯ

В статті розглянуті питання підвищення надійності газоперекачувальних агрегатів (ГПА) та компресорних установок (КУ). Використання викладеного математичного апарата в системах моніторингу газоперекачувальних агрегатів чи газотранспортних мереж дозволить побудову інтелектуальних автоматизованих систем керування.

1. Вступ

Над проблемою підвищення надійності газоперекачувальних агрегатів (ГПА) та компресорних установок (КУ) працюють академічні, галузеві науково-дослідні й проектно-конструкторські організації, вищі навчальні заклади, науково-виробничі та інші підприємства. Для її вирішення розгорнуті фундаментальні й прикладні дослідження.

Перехід на прогресивну систему експлуатації за станом, передбачає широке використання методів та засобів технічної діагностики. Реалізація цього стратегічного направлення розвитку газової промисловості диктує необхідність першочергового рішення питань діагностування ГПА та КУ – однієї з актуальних проблем сучасної науки про газотранспортні процеси.